REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Amendments to the Specification

The title has been amended and is now believed to be descriptive and clearly indicative of the invention to which the claims are directed.

The description has been amended to fix several clerical errors on pages 6 and 7. Numeral 30 on page 6, line 25 has been changed to 24, and numeral 30 on page 7, line18 has been changed to 20, consistent with the remainder of the description.

The specification was objected to under 37 CFR 1.75(d)(1) and MPEP § 608.01(o) for failing to provide proper antecedent basis for: "removably coupled to said personalized device" as stated in claim 12. A statement supporting this subject matter has been added to the description at page 6, line 19. The subject matter of claim 12 was present in the application as originally filed. Therefore, no new subject matter has been added.

The Applicant notes that the word "system" found on line 1 of claims 5 – 9 was corrected to read "method".

Claim Objections

Claims 5 and 8 were objected to because the word "favorable" was misspelled. Appropriate correction has been made, as reflected in the claim amendments above.

Claim 12 was objected to because the specification does not teach that the secure module is adapted to be "removably coupled to said personalized device". As indicated above, the necessary support has been added to the description.

Claim Rejections

Claim 6 was rejected under 35 U.S.C. 112, second paragraph as being indefinite due to the expression "said output" on line 31. Accordingly, the expression "said output" has been amended to read "said second output", which is introduced in claim 1.

Claims 1, 2, and 4-12 were rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,917,913 to Wang. The Applicant respectfully traverses this rejection.

The present application describes and claims a method for verifying data integrity in cryptographic schemes. As exemplified in the description, at least one correspondent in a cryptographic scheme uses a personalized device that has a main processor and a secure module. The secure module is adapted to operate independently of the main processor so that the internal state of the secure module can not be readily reverse engineered and/or that its interactions with the underlying hardware are not maliciously intercepted and reinterpreted (see page 6, line 14-19).

An exemplary method is outlined in the description on page 7, lines 14-26. Data that is to be verified is assembled, and two separate outputs are displayed, one by the main processor and one by the secure module. The secure module is then only instructed to generate a signature upon a favorable comparison of the two outputs. Since the two outputs are operably independent, a favorable comparison indicates data integrity to an entity who wishes to verify the integrity. The steps of claim 1 provide the above functionality.

The Applicant notes that claim 1 has been amended to remove the term "public-key" on line 2. Various other amendments were made to claim 1 to clarify the operation of the method.

Wang teaches a method in a portable electronic authorization device for approving a transaction request originated from an electronic transaction system. The method includes first receiving a first set of digital data at the portable electronic authorization device, wherein the first set of digital data represents the transaction request. The method then includes transmitting a second set of digital data to the electronic transaction system if the transaction request is approved by a use of the portable electronic authorization device. The second set of digital data is encrypted by an appropriate module in the portable electronic authorization device that signifies the user's approval of the transaction request.

Therefore, Wang teaches a single output, which is approved by a user before being sent to the electronic transaction system. Wang does not teach generating, displaying, or comparing two outputs to determine data integrity before approving the transaction. There is only a single output, sent along a single path. The Examiner points to col. 6, lines 35-48 of Wang as an

equivalent to the comparison of two outputs. The Applicant respectfully disagrees. In the passage indicated by the Examiner, Wang refers to an approval step based on a single output, and does not involve comparing two displayed outputs for determining data integrity. Therefore, Wang does not teach two outputs displayed separately by a main processor and a secure module respectfully, let alone the comparison of the two inputs to determine data integrity. Wang teaches an entirely different method than claim 1.

Moreover, Wang describes the encryption logic 300 as integrally operable with the device 200. Therefore, Wang also does not teach a secure module being independent of a main processor. Wang is entirely silent in that regard. In fact, such independence would not be required since Wang teaches only a single output and does not compare two outputs to determine data integrity.

Accordingly, Wang does not teach all the elements of claim 1. Specifically, Wang does not produce two different outputs that are displayed and compared in order to determine data integrity, and Wang does not teach a secure module being independent of a main processor.

Therefore, the Applicant believes that claim 1 clearly and patentably distinguishes over Wang, and as such is in condition for allowance. Claims 2-9 are either directly or indirectly dependent on claim 1, and as such, are also believed to distinguish over Wang.

Claim 10 was also rejected under 35 U.S.C. 102(b) in view of Wang. Claim 10 also incorporates the provision of a pair of outputs, the comparison of these outputs to determine data integrity, and the operable independence of a main processor and a secure module. Therefore, the Applicant submits that claim 10 also distinguishes over Wang, and as such is in condition for allowance. Claim 11 is dependent on claim 10, and therefore, is also believed to distinguish over Wang. The Applicant notes that claim 10 has been amended to replace the term "secure" with "trusted" consistent with the terminology used on page 6, line 30. Claim 10 has also been amended, replacing "PKI" with "cryptographic", and various amendments were made to clarify the operation of the method, consistent with claim 1.

Claim 12 was also rejected under 35 U.S.C. 102(b) in view of Wang. Claim 12 has been amended to include the comparison of data from a main processor and a secure module, which are operably independent, consistent with claims 1 and 10. Therefore, the Applicant submits that

amended claim 12 also distinguishes over Wang, and as such, is in condition for allowance. The Applicant notes that claim 12 has also been amended to correct various grammatical errors.

The Examiner rejected claim 3 under 35 U.S.C. 103(a) as being unpatentable over Wang, in view of WO 00/54457 to Vatanen. The Applicant respectfully traverses this rejection.

Vatanen teaches a mobile station for implementing a secure transaction having a communication network, service provider, and a mobile station interconnected with each other. The system described by Vatanen is used for accepting and processing electronically implemented transactions. Vatanen does not teach a pair of displayed inputs that are compared with each other, or an independently operable main processor and secure module. Therefore, Vatanen does not disclose the missing steps from Wang. The combination of Wang and Vatanen, therefore, does not teach all of the steps or features of the method described in claim 3 let alone claims 1-2, and 4-12. Accordingly, the Applicant submits that claims 1-12 clearly and patentably distinguish over the references cited by the Examiner, and as such are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,

John R.S. Orange
Agent for Applicant
Registration No. 29,725